O'NEILL CAREER HUB

How to Spot Fraudulent Internship/Job Postings

These "red flags" in no way cover all possible instances of fraud or all the red flags. Therefore, please always use your own discretion when applying to a position or interacting with a potential employer. Fraudulent job postings try to take your money, personal information, or both. The jobs often appear easy and convenient ways to make money with very little effort.

The following "red flags" are general markers to help you conduct a safer job search and protect your identity.:

Personal and Financial Information

- You are asked to provide your credit card, bank account numbers, or other personal financial documentation. Do NOT give out any financial information at any point during your job search and hiring process.
- The position requires an initial investment, such as a payment by wire service or courier.
- You are offered a large payment or reward in exchange for allowing the use of your bank account (often for depositing checks or transferring money).
- You are asked to provide your social security and driver's license information in the initial application. Personal information should never be asked during the initial application process.
- You are asked to provide a photo of yourself.

Job Posting

- The posting appears to be from a reputable, familiar company (often a Fortune 500). Yet, the email handle in the contact's email address does not match the domain used by representatives of the company (this is typically easy to determine from the company's website). Another way to validate is to check the open positions on the company's website, by checking their careers/jobs page.
- The posting includes spelling and grammatical errors.
- The posting neglects to mention the responsibilities of the job. Instead, the description focuses on the amount of money to be made.
- The position indicates a "first-year compensation" that is in high excess to the average compensation for that position type. The salary range listed is very wide (e.g., "employees can earn from $40K – $80K the first year!").

Contact and Communication

- Look at the company's website. Does it have an index that tells you what the site is about; or does it contain information only about the job in which you are interested? Scammers often create quick, basic web pages that seem legitimate at first glance.
- The contact email address contains the domain @live.com or an @ that is not affiliated with the company. Example: @gmail, @yahoo, @hotmail, etc.

- Watch for anonymity. If it is difficult to find an address, actual contact, company name, etc., this is cause to proceed with caution. Fraud postings are illegal, so scammers will try to keep themselves well hidden.
- When you Google the company name and the word "scam" (e.g., Acme Company Scam), the results show several scam reports concerning this company. Another source for scam reports is http://www.ripoffreport.com.
- Google the employer's phone number, fax number, and/or email address. If it does not appear connected to an actual business organization, this is a red flag. You can use the Better Business Bureau, Hoovers and AT&T's Anywho to verify organizations.
- The employer contacts you by phone, but there is no way to call them back (the number is not available).
- The employer tells you that they do not have an office set up in your area and will need you to help them get it up and running (these postings often include a request for your banking information, supposedly to help the employer make transactions).

Interview

- The interview is conducted online, via chat and an offer is given almost immediately.
- The employer responds to you immediately after you submit your resume. Typically, resumes sent to an employer are reviewed by multiple individuals or not viewed until the posting has closed. Note: this does not include an auto-response you may receive from the employer once you have sent your resume.

If Already Involved in a Scam

If you have encountered a fraudulent posting, company or organization, please contact the Career Hub at 812-855-9639 or email careerhb@indiana.edu so the posting can be investigated and appropriate action can be taken.

Interviewing Scams

Follow these safety tips when going on an interview:

- Always ensure it is in a public place and that someone knows of your plans to interview and the location.
- **If your instincts tell you it's suspicious, it probably is.**
- Do not feel pressured to give personally identifiable information in an application if you are not comfortable during an interview or during online/phone correspondence.
- Ask to take the document with you to complete and return so you have time to research the issue further. To learn more about employment scams, your rights, and appropriate actions, please visit this helpful page from the Riley Guide: http://www.rileyguide.com/scams.html